بسم الله الرحمن الرحيم

والحمد لله رب العالمين

والصلاة والسلام على سيدنا محمد النبي الكريم وعلى آله وأصحابه أجمعين

ربنا تقبل منا إنك أنت السميع العليم وتب علينا إنك أنت التواب الرحيم



يقول الله في كتابه العزيز

بِسْمِ اللَّهِ الرَّحْمَٰنِ الرَّحِيمِ

" وَمَا أُوتِيتُم مِّنَ الْعِلْمِ إِلَّا قَلِيلًا "

صَدَقَ اللَّهُ الْعَظِيمُ

"رب أشرح لي صدري ويسر لي أمرى واحلل عقدة من لسانى يفقهوا قولي"

اللهم لا علم لنا إلا ما علمتنا إنك أنت العليم الحكيم

أخوكم في الله

م / مصطفى عبده توفيق محمد

جمهورية مصر العربية

كيـــــــف تعمل الفيروسات

Mostafa Digital

كيف تعمل الفيروسات

الخطوة الأولى في مكافحة فيروسات الكمبيوتر، هي فهم أنواعها وآليات عملها

تتضمن معظم الكمبيوترات الشخصية المباعة حديثاً برامج لمكافحة الفيروسات، وهذه الحقيقة، أكثر من أي شيء آخر، تدلنا على مدى انتشار الفيروسات، ومدى قبول صناعة الكمبيوتر بها، كقدر لا مفر منه! لقد أصبحت الفيروسات أمراً واقعاً في عالم الكمبيوتر اليوم.يوجد حالياً الآلاف من فيروسات الكمبيوتر، ويمكن تصنيفها إلى عدة فئات، لكنها جميعاً، على العموم، تخضع لتعريف مشترك بسيط: الفيروس هو برنامج كمبيوتر مصمم عمداً ليقترن ببرنامج آخر، بحيث يعمل الفيروس عندما يعمل ذلك البرنامج، ومن ثمَّ يعيد إنتاج نفسه باقترانه ببرامج أخرى. ويقترن الفيروس بالبرنامج الأصلي بإلصاق نفسه به، أو باستبداله أحياناً، وقد يغير الفيروس نفسه عند إعادة الإنتاج، فيظهر كنسخة معدلة عن النسخة التي قبلها، كلما كرر العملية. ويمكن أن تتلوث برامج الماكرو بالفيروس، أو قطاع الإقلاع (boot sector) على القرص، وهو أول برنامج يتم تحميله من قرص يحمل ملفات إقلاع نظام التشغيل.

لاحظ عبارة "مصمم عمداً" في التعريف، فالفيروسات لا تظهر صدفة، بل يكتبها مبرمجون ذوو مهارات عالية عادة، ثم يجدون طريقة لنشرها في أجهزة المستخدمين الغافلين عنها. وكلما أصبحت برامج مكافحة الفيروسات أقوى، زاد المبرمجون من جهودهم لتطوير فيروسات أذكى، للتحايل عليها. والهدف من تطوير الفيروسات، بالنسبة للكثير من مؤلفيها، ليس أكثر من تحد، والرغبة في إثبات تفوقهم، بينما هو للبعض الآخر التلذذ بإثارة حيرة الآخرين وشكوكهم في الكمبيوتر، أو إزعاجهم، وحتى إيذائهم! وهذا أمر

سيئ جداً، إذ يمكنهم أن يجنوا أموالاً طائلة، إذا وجهوا مواهبهم لمساعدة الشركات على حل مشكلة العام 2000، بدلاً من هدرها في أعمال لا طائل منها، مثل تطوير الفيروسات.

اشتهرت فيروسات الكمبيوتر بقدرتها على الأذى وإحداث الأضرار، لكن في الحقيقة، فإن الكثير منها غير مؤذ. صحيح أن بعضها يحذف الملفات، أو يقوم بأعمال تخريبية أخرى، لكن معظمها يسبب إزعاجاً بسيطاً فقط، وبعضها لا يلحظه المستخدم العادي أبداً. ويكفي أن يتمكن البرنامج من إعادة إنتاج نفسه حتى يعتبر فيروساً، بغض النظر عن الأعمال التي ينفذها.

لكن، في الحقيقة، حتى الفيروسات غير المؤذية، تسبب بعض الأذى! فهي تستهلك مساحات تخزين على القرص، وجزءاً من ذاكرة الكمبيوتر، وتشغل جزءاً من طاقة المعالج، وبالتالي فهي تؤثر على سرعة وكفاءة الجهاز. أضف إلى ذلك، أن برامج كشف الفيروسات وإزالتها، تستهلك أيضاً موارد الجهاز. ويرى الكثير من المستخدمين، أن برامج مكافحة الفيروسات تبطئ عمل الجهاز بشكل ملحوظ، وهي أكثر تطفلاً عليه من الفيروسات ذاتها! وبعبارة أخرى، تؤثر الفيروسات في عالم الكمبيوتر، حتى إذا لم تكن تفعل شيئاً.

الفيروسات وأشباه الفيروسات

إن الشرح المذكور في الفقرة السابقة عن الفيروس، أكثر تحديداً من الطريقة التي نستخدم فيها كلمة "فيروس" في الواقع. وتوجد أنواع أخرى من البرامج، ينطبق عليها تعريف الفيروس جزئياً. تشترك هذه الأنواع مع الفيروسات في أنها تعمل بدون علم المستخدم، وتقوم بأعمال ضمن الكمبيوتر، مصممة عمداً لتنفيذها. ومن هذه الأنواع: الديدان (worms)، وأحصنة طروادة (horses Trojan)، وبرامج الإنزال (droppers). وتعتبر كل هذه البرامج، بما فيها الفيروسات، جزءاً من فئة أكبر تدعى البرامج الماكرة (malware)، وهي مشتقة من عبارة malicious-logic software.

والدودة برنامج يعيد إنتاج نفسه، لكنها لا تلوث برامج أخرى. تنسخ الدودة نفسها من وإلى الأقراص المرنة، أو عبر الشبكات، ويعتمد بعضها على الشبكة في إنجاز عملها. تستخدم إحدى أنواع الديدان –وهي الدودة المضيفة (host worm)– الشبكة لنسخ نفسها، فقط، إلى أجهزة الكمبيوتر المتصلة بالشبكة. بينما توزع الدودة الشبكية (network worm) أجزاءها على عدة كمبيوترات، وتعتمد على الشبكة فيما بعد لتشغيل هذه الأجزاء. ويمكن أن تظهر الديدان على كمبيوترات منفصلة، فتنسخ نفسها إلى أماكن متعددة على القرص الصلب.

وسمي النوع الثاني من البرمجيات الماكرة "حصان طروادة"، نسبة للأسطورة الإغريقية الواردة في ملحمة الأوديسا لهوميروس، حيث ترك الجيش الإغريقي حصاناً خشبياً ضخماً، كهدية لسكان طروادة، وكان يختبئ ضمنه مجموعة من الجنود الأشداء، بعد أن تظاهروا بإنهاء الحصار الطويل، وعندما رحل الجيش وأدخل السكان الحصان إلى داخل أسوار المدينة، خرج الجند منه وانقضوا على الحامية، وسقطت المدينة في أيدي الإغريق. وتعتمد برامج أحصنة طروادة على المبدأ ذاته، فهي تختبئ ضمن برامج يبدو مظهرها بريئاً، وعندما يشغّل المستخدم واحداً من هذه البرامج، ينشط الجزء الماكر ويقوم بعمل معين مصمم له. وتختلف أحصنة طروادة عن الفيروسات العادية، في أنها لا تعيد إنتاج نفسها.

وصممت برامج الإنزال (droppers) لمراوغة برامج مكافحة الفيروسات، وتعتمد على التشفير غالباً لمنع اكتشافها. ووظيفة هذه البرامج عادة، نقل وتركيب الفيروسات، فهي تنتظر لحظة حدوث أمر معين على الكمبيوتر، لكي تنطلق وتلوثه بالفيروس المحمول في طياتها.

وينتمي مفهوم قنبلة (bomb) الكمبيوتر إلى هذه الفئة، إذ تبنى القنابل ضمن البرمجيات الماكرة كواسطة لتنشيطها. وتبرمج القنابل لتنشط عند حدوث حدث معين. تنشط بعض القنابل في وقت محدد، اعتماداً على ساعة الكمبيوتر. فيمكن برمجة قنبلة مثلاً، لمسح كافة الملفات ذات الامتداد .DOC من قرصك الصلب، عشية رأس السنة الميلادية، أو لعرض رسالة على الشاشة، في اليوم المصادف لعيد ميلاد شخصية مشهورة. وتعمل بعض القنابل تحت شروط أو أحداث أخرى، فيمكن أن تنتظر القنبلة إلى أن يتم تشغيل برنامج معين، عشرين مرة مثلاً، وعندها تمسح ملفات القوالب (templates) الخاصة بهذا البرنامج. ومن وجهة النظر هذه، تعتبر القنابل مجرد برامج جدولة زمنية ماكرة.

ويمكننا النظر إلى الفيروسات كحالات خاصة من البرمجيات الماكرة، إذ يمكن للفيروسات الانتشار بواسطة برامج الإنزال (ولا يشترط ذلك)، وهي تستخدم مفهوم برامج الديدان لإعادة إنتاج نفسها. ولا تعتبر الفيروسات مماثلة لأحصنة طروادة من الناحية التقنية، إلا أنها تشابهها في نقطتين: فهي تنفذ أعمالاً لا يريدها المستخدم، وتحول البرنامج الذي تلتصق به إلى حصان طروادة عملياً (تختبئ داخله، وتعمل عندما يعمل البرنامج، وتنفذ أعمالاً غير مرغوبة)

كيف يعمل الفيروس؟

تعمل الفيروسات بطرق مختلفة، وسنعرض فيما يلي الطريقة العامة التي تنتهجها كافة الفيروسات. في البداية يظهر الكمبيوتر على جهازك، ويكون قد دخل إليه مختبئاً في ملف برنامج ملوث (مثل ملفات COM أو EXE أو قطاع الإقلاع). وكانت الفيروسات في الماضي تنتشر بشكل أساسي عن طريق توزيع أقراص مرنة ملوثة. أما اليوم، فمعظمها يأتي مع البرامج المنقولة عبر الشبكات (ومن بينها إنترنت)، كجزء من برنامج تركيب نسخة تجريبية من تطبيق معين، أو ماكرو لأحد التطبيقات الشهيرة، أو كملف مرفق (attachment) برسالة بريد إلكتروني.

ويجدر التنويه إلى أن رسالة البريد الإلكتروني نفسها لا يمكن أن تكون فيروساً، فالفيروس برنامج، ويجب تشغيله لكي يصبح نشطاً. إذاً الفيروس المرفق برسالة بريد إلكتروني، لا حول له ولا قوة، إلى أن تشغّله. ويتم تشغيل فيروسات المرفقات عادة، بالنقر عليها نقرة مزدوجة بالماوس. ويمكنك حماية جهازك من هذه الفيروسات، بالامتناع عن تشغيل أي ملف مرفق برسالة بريد إلكتروني، إذا كان امتداده COM أو EXE، أو إذا كان أحد ملفات بيانات التطبيقات التي تدعم الماكرو، مثل برامج أوفيس، إلى ما بعد فحصه والتأكد من خلوه من الفيروسات. أما ملفات الرسوميات والصوت، وأنواع ملفات البيانات الأخرى القادمة كمرفقات، فهي آمنة، ولا يمكن للفيروس أن ينشط من خلالها، ولذلك فهو لا يهاجمها.

إذاً يبدأ الفيروس دورة حياته على الجهاز بشكل مشابه لبرنامج حصان طروادة، فهو يختبئ في ثنايا برنامج أو ملف آخر، وينشط معه. في الملفات التنفيذية الملوثة، يكون الفيروس قد أضاف شيفرته إلى البرنامج الأصلي، وعدل تعليماته بحيث ينتقل التنفيذ إلى شيفرة الفيروس. وعند تشغيل الملف التنفيذي المصاب، يقفز البرنامج عادة إلى تعليمات الفيروس، فينفذها، ثم يعود ثانية لتنفيذ تعليمات البرنامج الأصلي. وعند هذه النقطة يكون الفيروس ناشطاً، وجهازك أصبح ملوثاً.

وقد ينفذ الفيروس مهمته فور تنشيطه (ويطلق عليه فيروس العمل المباشر (direct-action)، أو يقبع منتظراً في الذاكرة، باستخدام وظيفة "الإنهاء والبقاء في الذاكرة" terminate and stay resident, TSR)، التي تؤمنها نظم التشغيل عادة. وتنتمي غالبية الفيروسات لهذه الفئة، ويطلق عليها الفيروسات "المقيمة". ونظراً للإمكانيات الكبيرة المتاحة للبرامج المقيمة في الذاكرة، بدءاً من تشغيل التطبيقات والنسخ الاحتياطي للملفات إلى مراقبة ضغطات لوحة المفاتيح ونقرات الماوس (والكثير من الأعمال الأخرى)، فيمكن

برمجة الفيروس المقيم، لتنفيذ أي عمل يمكن أن يقوم به نظام التشغيل، تقريباً. يمكن تشغيل الفـــيروس المقـــيم كقنبلة، فيبدأ مهمته على جهازك عند حدث معين. ومن الأمور التي تستطيع الفيروسات المقيمة عملها، مسح (scan) قرصك الصلب وأقراص الشبكة بحثاً عن الملفات التنفيذية، ثم نسخ نفسها إلى هذه الملفات وتلويثها.

أنواع الفيروسات

يبحث مطورو الفيروسات، بشكل دائم، عن طرق جديدة لتلويث كمبيوترك، لكن أنواع الفيروسات معدودة عملياً، وتصنف إلى: فيروسات قطاع الإقلاع (boot sector viruses)، وملوثات الملفات (file infectors)، وفيروسات الماكرو (macro viruses). وتوجد أسماء أخرى لهذه الفئات، وبعض الفئات المتفرعة عنها، لكن مفهومها يبقى واحداً.

تقبع فيروسات قطاع الإقلاع في أماكن معينة على القرص الصلب ضمن جهازك، وهي الأماكن التي يقرأها الكمبيوتر وينفذ التعليمات المخزنة ضمنها، عند الإقلاع. تصيب فيروسات قطاع الإقلاع الحقيقية منطقة قطاع الإقلاع الخاصة بنظام دوس (DOS boot record)، بينما تصيب فيروسات الفئة الفرعية المسماة MBR viruses، قطاع الإقلاع الرئيسي للكمبيوتر (master boot record). يقرأ الكمبيوتر كلا المنطقتين السابقتين من القرص الصلب عند الإقلاع، مما يؤدي إلى تحميل الفيروس في الذاكرة. يمكن للفيروسات أن تصيب قطاع الإقلاع على الأقراص المرنة، لكن الأقراص المرنة النظيفة، والمحمية من الكتابة، تبقى أكثر الطرق أمناً لإقلاع النظام، في حالات الطوارئ. والمشكلة التي يواجهها المستخدم بالطبع، هي كيفية التأكد من نظافة القرص المرن، أي خلوه من الفيروسات، قبل استخدامه في الإقلاع، وهذا ما تحاول أن تفعله برامج مكافحة الفيروسات.

تلصق ملوثات الملفات (وتدعى أيضاً الفيروسات الطفيلية (parasitic viruses) نفسها بالملفات التنفيذية، وهي أكثر أنواع الفيروسات شيوعاً. وعندما يعمل أحد البرامج الملوثة، فإن هذا الفيروس، عادة، ينتظر في الذاكرة إلى أن يشغّل المستخدم برنامجاً آخر، فيسرع عندها إلى تلويثه. وهكذا، يعيد هذا النوع من الفيروس إنتاج نفسه، ببساطة، من خلال استخدام الكمبيوتر بفعالية، أي بتشغيل البرامج! وتوجد أنواع مختلفة من ملوثات الملفات، لكن مبدأ عملها واحد.

تعتمد فيروسات الماكرو (macro viruses)، وهي من الأنواع الحديثة نسبياً، على حقيقة أن الكثير من التطبيقات تتضمن لغات برمجة مبيتة ضمنها. وقد صممت لغات البرمجة هذه لمساعدة المستخدم على أتمتة العمليات المتكررة التي يجريها ضمن التطبيق، من خلال السماح له بإنشاء برامج صغيرة تدعى برامج الماكرو. تتضمن برامج طاقم أوفيس، مثلاً، لغة برمجة مبيتة، بالإضافة إلى العديد من برامج الماكرو المبيتة أيضاً، والجاهزة للاستخدام المباشر. وفيروس الماكرو ببساطة، هو برنامج ماكرو مصمم للعمل مع تطبيق معين، أو عدة تطبيقات تشترك بلغة برمجة واحدة. أصبحت فيروسات الماكرو شهيرة بفضل الفيروس المصمم لبرنامج

مايكروسوفت وورد. فعندما تفتح وثيقة أو قالباً ملوثين، ينشط الفيروس ويؤدي مهمته التخريبية. وقد بُرمِج هذا الفيروس لينسخ نفسه إلى ملفات الوثائق الأخرى، مما يؤدي إلى ازدياد انتشاره مع استمرار استخدام البرنامج.

ويجمع نوع رابع يدعى الفيروس "متعدد الأجزاء" (multipartite) بين تلويث قطاع الإقلاع مع تلويث الملفات، في وقت واحد.

ستجد قائمة ضخمة بأسماء الفيروسات، مع شرح تفصيلي عن آثار كل منها، في قسم Virus Encyclopedia من موقع مختبر مكافحة الفيروسات، الخاص بشركة سيمانتك، على العنوان: http://www.symantec.com/avcenter/vinfodb.html

ذكاء الفيروسات في ازدياد

نجح مبدأ فيروس الماكرو، لأن لغات البرمجة أمنت إمكانية الوصول إلى الذاكرة والأقراص الصلبة. وهذا ما أمنته التقنيات الحديثة أيضاً، بما فيها عناصر تحكم ActiveX، وبرمجيات جافا (Java applets). صحيح أن هذه التقنيات صُممت مع ضمان حماية القرص الصلب من برامج الفيروسات (تعد جافا أفضل من ActiveX في هذا المجال)، لكن الحقيقة أن هذه البرامج تستطيع تركيب نفسها على جهازك بمجرد زيارتك لموقع ويب. ومن الواضح أن أجهزتنا ستكون أكثر عرضة لمخاطر الفيروسات والبرمجيات الماكرة الأخرى، مع ازدياد تشبيك الكمبيوترات ببعضها، وبشبكة إنترنت، خصوصاً مع المزايا التي تعدنا بها إنترنت لإجراء ترقية نظم التشغيل عبرها (يؤمن نظاما ويندوز98 وويندوز2000 هذه الإمكانيات).

إن أقل ما يوصف به مطورو الفيروسات، هو مهارتهم وقدرتهم الفذة على الابتكار، فهم يخرجون إلينا دائماً بطرق جديدة لخداع برامج مكافحة الفيروسات. فمثلاً، تضلل الفيروسات المتسللة (stealth viruses) الجديدة، برامج مكافحة الفيروسات، بإيهامها أن الأمور تسير على ما يرام، ولا يوجد أي مؤشر على وجود فيروس. كيف؟

يعتمد مبدأ عمل الفيروس المتسلل، على الاحتفاظ بمعلومات عن الملفات التي لوثها، ثم الانتظار في الذاكرة، ومقاطعة عمل برامج مكافحة الفيروسات خلال بحثها عن الملفات المعدلة، وإعطائها المعلومات القديمة التي يحتفظ بها عن هذه الملفات، بدلاً من السماح لها بالحصول على المعلومات الحقيقية من نظام التشغيل!

أما الفيروسات متغيرة الشكل (viruses polymorphic)، فتعدل نفسها أثناء إعادة الإنتاج، مما يجعل من الصعب على برامج مكافحة الفيروسات التي تبحث عن نماذج معينة من مثل هذا الفيروس، اكتشاف كافة أشكاله الموجودة، وبالتالي تستطيع الفيروسات الناجية، الاستمرار وإعادة إنتاج أشكال جديدة.

تظهر أنواع جديدة من الفيروسات إلى حيز الوجود بشكل دائم، مع استمرار لعبة القط والفأر بين مطوري الفيروسات ومنتجي برامج مكافحتها. وأغلب الظن أن الفيروسات ظهرت لتبقى، إلى ما شاء الله.

بعض الفيروسات الشائعة

اسم الفيروس	نوعه	مجالات التلويث	مواصفاته
Aol4free.com	حصان طروادة	لا شيء! فهو يحذف الملفات من القرص الصلب، لكنه لا ينتقل إلى تطبيقات أخرى	يستخدم تعليمة Deltree (من دوس) عند تنشيطه، لحذف الملفات من القرص الصلب، وهو مختلف عن فيروس Aol4free السابق له
Form	مقيم، قطاع الإقلاع	قطاع الإقلاع على الأقراص المرنة	قديم نسبياً لكنه شائع، يصدر صوت نقرات عند الضغط على لوحة المفاتيح
Hare	مقيم، متغير الشكل، متعدد الأجزاء	ملفات COM و EXE، وقطاع الإقلاع الرئيسي، وقطاع الإقلاع على الأقراص المرنة	ينشط في الثاني والعشرين من أغسطس وسبتمبر، ويحاول مسح سواقات :A و :B و :C
Java.App Strange Brew	ملوث ملفات، مباشر العمل	ملفات فئات جافا	أول فيروس يصيب بريمجات جافا، ويمكنه الانتشار عبر نظم تشغيل مختلفة، لكن لا تعرف له أضرار
Microsoft.Excel.Spellcheck	ماكرو	جداول إكسل الممتدة	يشكل الملف Spellck.xla في مجلد إقلاع إكسل، وهو غير مؤذ، لكنه يعرض رسائل يحذر فيها من فيروسات الماكرو
Monica (Hanko.4167)	ملوث ملفات، متسلل، مقيم	ملفات COM و EXE	يوقف عمل الكمبيوتر في الساعة السابعة وسبع دقائق، في اليوم السابع من شهر يوليو، أي 7/7-7:07، ويظهر كلمة Monica
W95.CIH	ملوث ملفات، مقيم	ملفات EXE لويندوز95	ينشط في السادس والعشرين من كل شهر، ويحاول الكتابة فوق ذاكرة فلاش بيوس، وتخريب بيانات القرص الصلب
W95.Marburg	ملوث ملفات، مباشر العمل	ملفات التطبيقات لنظم ويندوز95/98/إن.تي	ينشط بعد ثلاثة أشهر من أول إصابة به، فعند تشغيل تطبيق ملوث، يغطي الشاشة بأيقونة الخطأ في ويندوز، ويحذف برامج مكافحة الفيروسات
W97/X97M Shiver	ماكرو	وثائق (ملفات بيانات) وورد97 وإكسل97	أول فيروس من نوع الماكرو يصيب ملفات وورد وإكسل معاً، ويمنع تحميل الوثائق الملوثة
Win32/Semisoft	ملوث ملفات، مقيم	ملفات EXE لنظم ويندوز	يرسل معلومات من عدة ملفات على القرص الصلب، إلى عناوين IP محددة، عبر إنترنت
WM.PolyPoster	ماكرو	وثائق وورد	يرسل رسالة إلى مجموعات نقاش محددة، بواسطة برنامج Free Agent، ويضع وثيقة وورد الراهنة كملف مرفق بالرسالة
XM.Compat	ماكرو، متغير الشكل	جداول إكسل الممتدة	ينشط بعد تاريخ 31 أغسطس 1998 عند إغلاق جدول ملوث، فيختار مجموعة عشوائية من الخلايا العددية، ويغير قيمها بنسبة 5 بالمائة.





أرجو أن تكونوا استفدتم بقراءة هذا الكتاب ولتدعوا الله لي بظهر الغيب

ولأي استفسار بالرجاء مراسلتي على الرابط التالي :-

E mail :- MostafaDigital@yahoo!.com

ولكم تحياتي
م/ مصطفى عبده توفيق محمد